Journal of Information Assurance and Security
ISSN 1554-1010 Volume 6 (2011) pp. 195-215

A Comparison of Routing Attacks on Wireless Sensor Networks

Shahriar Mohammadi[1]; Reza Ebrahimi Atani[2, 3] and Hossein Jadidoleslamy[3]

[1] Information Technology Engineering Group, Department of Industrial Engineering,
K.N. Tossi University of Technology, Tehran, Iran
Smohammadi40@yahoo.com

[2] Department of Computer Engineering, The University of Guilan, P.O. Box 3756, Rasht, Iran,
rebrahimi@guilan.ac.ir

[3] Department of Information Technology, Anzali International Branch, The University of Guilan, Rasht, Iran
tanha.hossein@gmail.com

Abstract: **Wireless sensor networks (WSNs) have many potential applications [1, 5] and unique challenges. They usually consist of hundreds or thousands small sensor nodes such as MICA2, which operate autonomously; conditions such as cost, invisible deployment and many application domains, lead to small size and limited resources sensors [2]. WSNs are vulnerable to many types of routing attacks [1] and most of traditional networks security techniques are unusable on WSNs [2]; due to wireless and shared nature of communication channel, untrusted transmissions, deployment in open environments, unattended nature and limited resources [1]. So, security is a vital requirement for these networks; but we have to design a proper security mechanism that attends to WSN's constraints and requirements. In this paper, we focus on security of WSNs, divide it (the WSNs security) into four categories and will consider them, including an overview of WSNs, security in WSNs, the threat model on WSNs, a wide variety of WSNs' routing attacks and a comparison of them. This work enables us to identify the purpose and capabilities of the attackers; also, the goals and effects of the routing attacks on WSNs are introduced. Also, this paper discusses known approaches of detection and defensive mechanisms against the routing attacks; this would enable it security managers to manage the routing attacks of WSNs more effectively.**

Key words: wireless sensor network (WSN), security, routing, attacks, detection, defensive mechanism.

I. Introduction

Advances in wireless communications have enabled the development of low-cost and low-power wireless sensor networks (WSNs) [1]. WSNs have many potential applications [1, 5] and unique challenges. They usually are heterogeneous systems contain many small devices, called sensor nodes, that monitoring different environments in cooperative; i.e. sensors cooperate to each other and compose their local data to reach a global view of the environment; sensor nodes also can operate autonomously. In WSNs there are two other components, called "aggregation points" and "base stations" [3], which have more powerful resources than normal sensors. Aggregation points collect information from their nearby sensors, integrate them and then forward to the base stations to process gathered data, as shown in figure1. limitations such as cost, invisible deployment and variety application domains, lead to requiring small size and limited resources (like energy, storage and processing) sensors [2]. Also, WSNs are vulnerable to many types of attacks and due to unsafe and unprotected nature of communication channel [4, 9, 22], untrusted and broadcast transmission media, deployment in hostile environments [1, 5], automated nature and limited resources, the most of security techniques of traditional networks are impossible in WSNs; therefore, security is a vital and complex requirement for these networks. It is necessary to design an appropriate security mechanism for these networks [5, 6], which attending to be WSN's constraints. This security mechanism should cover different security dimension of WSNs, include confidentiality, integrity, availability and authenticity. The main purpose of this paper is presenting an overview of different routing attacks on WSNs and comparing them together. In this paper, we focus on security of WSNs and classify it into four categories, as follows:

- An overview of WSNs,
- Security in WSNs include security goals, security obstacles and security requirements of WSNs,
- The threat model on WSNs,
- A wide variety of WSN's routing attacks and comparison them to each other, include classification of WSN's routing attacks based on threat model and compare them to each other based on their goals, results, strategies, detection and defensive mechanisms;

This work makes us enable to identify the purpose and capabilities of the attackers; also, the goal, final result and effects of the attacks on the WSNs. We also state some available approaches of security detection and defensive mechanisms against these attacks to handle them. The rest of this paper is organized as follows: in section 2 is presented an overview of WSNs; while section 3 focused

on security in WSNs and presents a diagram about it; section 4 considers the threat model in WSNs; section 5 includes definitions, strategies and effects of routing attacks on WSNs; in section 6 is considered WSNs' routing attacks, their goals, effects, possible detection and defensive mechanisms, and extracts their different features, then classifies the routing attacks based on extracted features and compares them to each other; and finally, in section 7, we present our conclusion.

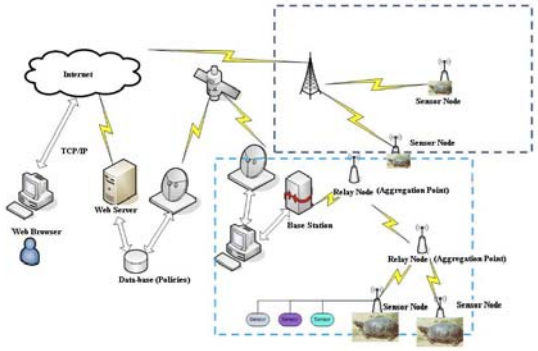


Figure1. WSN's architecture

II. Overview of WSNs

In this section, we present an outline of different dimensions of WSNs, such as definition, characteristics, applications, constraints and challenges; as presented in following subsections (subsection 2.1, 2.2, 2.3 and 2.4)

A. Definition and suppositions of WSNs

A WSN is a heterogeneous system consists of hundreds or thousands low-cost and low-power tiny sensors to monitoring and gathering information from deployment environment in real-time [6, 7, 8]. Common functions of WSNs are including broadcast and multicast, routing, forwarding and route maintenance. The sensor's components are: sensor unit, processing unit, storage/memory unit, power supply unit and wireless radio transceiver; these units are communicating to each other, as shown in following figure (figure2). The existing components on WSN's architecture are including sensor nodes (motes or field devices that are sensing data), network manager, security manager, aggregation points, base stations (access point or gateway) and user/human interface. Besides, there are two approaches in WSN's communication models containing hierarchical WSN versus distributed [6] and homogeneous WSN versus heterogeneous [6]. Some of common suppositions of these networks are:

- Insecure radio links [8, 9, 10],
- Packet injection and replay [8, 9],
- Non tamper resistant [10],
- Many normal sensor nodes (high-density) and low malicious nodes,
- Powerful attackers (laptop-class) [10, 20].

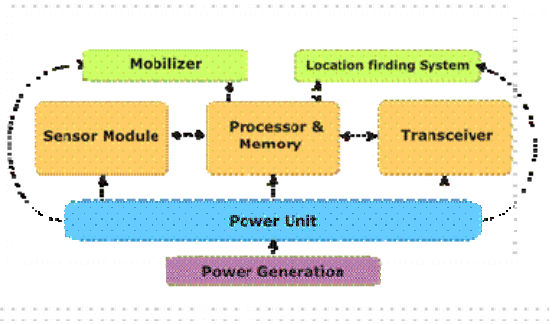


Figure2. WSN's node architecture

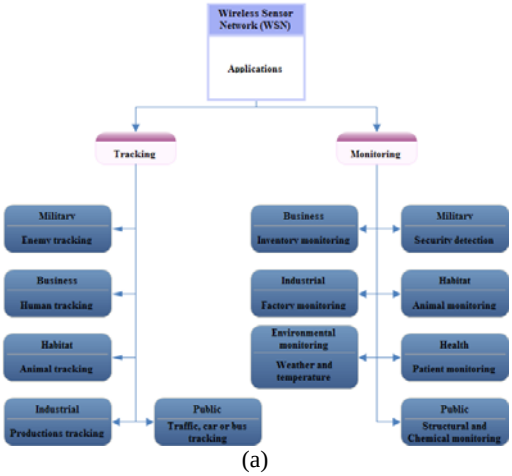
B. WSNs characteristics and weakness

Most important characteristics of WSNs are including:

- Constant or mobile sensors (mobility),
- Sensor limited resources [4, 18] (limited range radio communication, energy, computational capabilities [4]),
- Low reliability, wireless communication [4],
- Immunity,
- Dynamic/unpredictable WSN's topology and self-organization [4, 21],
- Ad-hoc based networks [8, 19],
- Hop-by-hop communication (multi-hop routing) [11, 12, 21],
- Non-central management,
- Autonomously, infrastructure-less [8],
- Open/hostile-environment nature [8, 10],
- High density;

C. WSN's applications

In general, there are two kinds of applications for WSNs including, monitoring and tracking [8]; therefore, some of most common applications of these networks are: military, medical, environmental monitoring [2, 6, 8], industrial, infrastructure protection [2, 8], disaster detection and recovery, agriculture, intelligent buildings, law enforcement, transportation and space discovery (as shown in figure3: a and b).



(a)

(b)

Figure3. WSN's applications

D. Vulnerabilities and challenges of WSNs

WSNs are vulnerable to many kinds of attacks; some of most important reasons are including:

- Theft (reengineering, compromising and replicating),
- Limited capabilities [13, 14] (DoS attacks risks, constraint in using encryption),
- Random deployment (hard pre-configuration) [13, 22],
- Unattended nature [13, 19, 21, 22];

In continue this section states most common challenges and constraints in WSNs; include:

- Deployment on open/dynamic/hostile environments [19, 20, 22] (physical access, capture and node destruction);
- Insider attacks;
- Inapplicable/unusable traditional security techniques [2, 14, 22] (due to limited devices/resources, deploying in open environments and interaction with physical environment);
- Ad-hoc based deployment [19, 20] (dynamic structure and topology, self-organization);
- Resource scarcity/hungry [4, 17, 22] (low and expensive communication/computation/processing resources);
- Immense/large scale (high density, scalable security mechanism requirement);
- Unreliable communication [4, 22] (connectionless packet-based routing ⇨ unreliable transfer, channel broadcast nature ⇨ conflicts, multi-hop routing and network congestion and node processing ⇨ Latency);
- Unattended operation [9, 20] (Exposure of physical attacks, managed remotely, no central management point);
- Redesigning security architectures (distributed and self-organized);
- Increased attacks' risks and vulnerabilities [22], new attacks, increased tiny/embedded devices, multi-hopping routing (selfish) [21];
- Devices with limited capabilities [15, 16], pervasiveness (privacy worries), wireless (medium) [4, 13, 22] and mobility;

III. Security in WSNs

At the moment, intrusion techniques in WSNs are growth; also there are many methods to disrupt these networks. In WSNs, data accuracy and network health are necessary; because these networks usually use on confidential and sensitive environments. There are three security key points on WSNs, including system (integrity, availability), source (authentication, authorization) and data (integrity, confidentiality). Necessities of security in WSNs are:

- Correctness of network functionality;
- Unusable typical networks protocols [2, 19];
- Limited resources [22, 24];
- Untrusted nodes [19, 20];
- Requiring trusted center for key management [19],
    - Authenticating nodes to each other [25];
    - Preventing from existing attacks and selfishness [24, 26];
    - Extending collaboration;

A. Why security in WSNs?

Security in WSNs is an important, critical issue, necessary and vital requirement, due to:

- WSNs are vulnerable against security attacks [22, 23] (broadcast and wireless nature of transmission medium);
- Nodes deploy on hostile environments [19, 20, 22] (unsafe physically);
- Unattended nature of WSNs [9, 20];

B. Security issues

This section states the most important discussions on WSNs; it is including:

- Key establishment,
- Secrecy,
- Authentication,
- Privacy,
- Robustness to DoS attacks,
- Secure routing, node capture [13, 19];

C. Security services

There are many security services on WSNs; but some of their common are including encryption and data link layer authentication [17, 19, 20, 24], multi-path routing [19, 21, 24, 25], identity verification, bidirectional link verification [19, 21, 25] and authenticated broadcasts.

D. Security protocols

This section presents the most common security protocols of WSNs, containing:

- SNEP: Secure network encryption protocol (secure channels for confidentiality, integrity by using authentication, freshness);
- µTESLA [6, 19] (Micro timed, efficient, streaming, loss-tolerant authentication protocol, authentication by using asymmetric authenticated broadcast);
- SPIN (Sensor protocols for information via negotiation): The idea behind SPIN is to name the data using high-level descriptors or meta-data. Before transmission, metadata are exchanged among sensors via a data advertisement mechanism, which is the key feature of SPIN. Each node upon receiving new data,

advertises it to its neighbors and interested neighbors, i.e. those who do not have the data, retrieve the data by sending a request message. There is no standard meta-data format and it is assumed to be application specific. There are three messages defined in SPIN to exchange data between nodes, include: ADV message to allow a sensor to advertise a particular meta-data, REQ message to request the specific data and DATA message that carry the actual data [11, 21];

- Broadcasts of end-to-end encrypted packets [24, 25] (authentication, integrity, confidentiality, replay);

As figure4 shows, the most important dimensions of security in WSNs are including security goals, obstacles, constraints, security threats, security mechanisms and security classes; however, this paper considers only star spangled parts/blocks to classify and compare WSNs' routing attacks based on them; i.e. security threats (including availability, authenticity, integrity and confidentiality) and security classes (containing interruption, interception, modification and fabrication); as shown in table3.

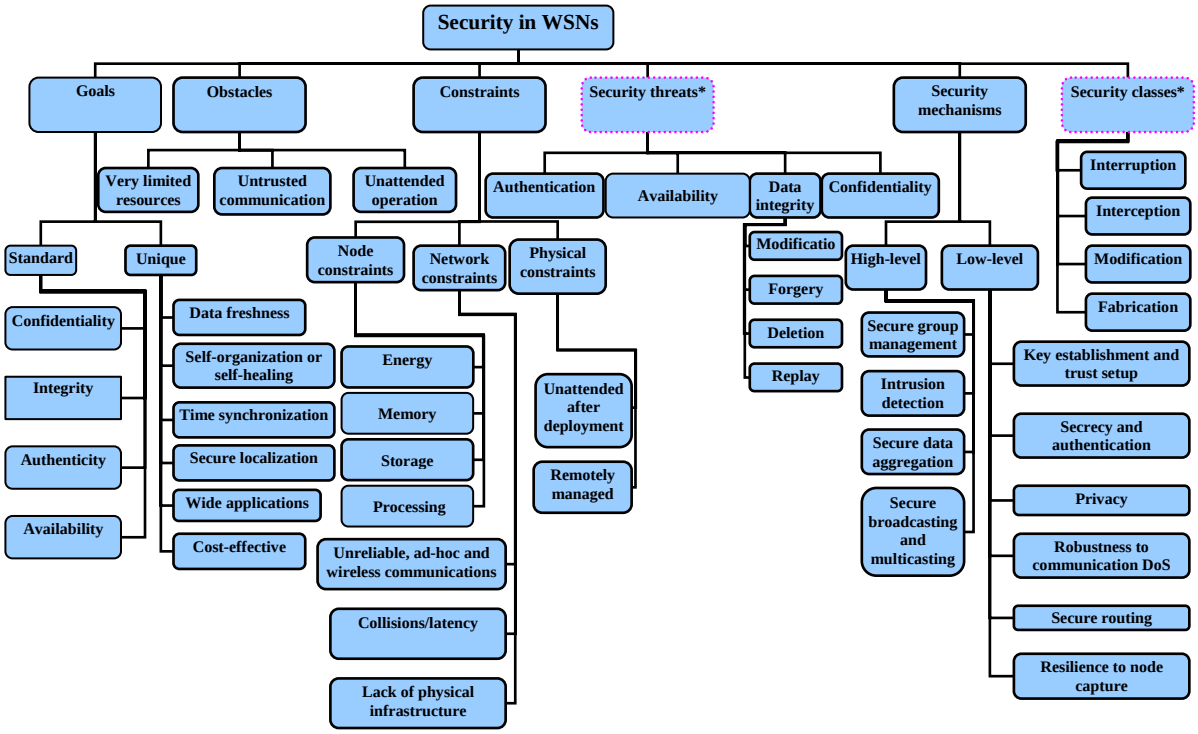


Figure4. Security in WSNs

IV. Threat model in WSNs

There are many classes of WSNs' attacks based on nature and goals of attacks or attackers; but, in this section we present and compare their most important classes (called threat model of WSNs); as presented in following subsections (subsection 4.1, 4.2, 4.3 and 4.4).

E. Attacks based on damage/access level

In this subsection is presented the classifications of WSNs' routing attacks based on their damage level or attacker's access level, including:

1) Active attacker: These kinds of attacker do operations, such as:

- Injecting faulty data into the WSN;
- Impersonating [2, 8];
- Packet modification [19];
- Unauthorized access, monitor, eavesdrop and modify resources and data stream;
- Creating hole in security protocols [20];
- Overloading the WSN;

Some of most goals and effects of these attacks are:

- The WSN functionality disruption;
- The WSN performance degradation;
- Sensor nodes destruction;
- Data alteration;
- Inability in use the WSN's services;
- Obstructing the operations or to cut off certain nodes from their neighbors;

2) Passive attacker: passive attacker may do following functions:

- Attacker is similar to a normal node and gathers information from the WSN;
- Monitoring and eavesdropping [2, 20] from communication channel by unauthorized attackers;
- Naturally against privacy;

The goals and effects of this kind of attacker include:

- Eavesdropping, gathering and stealing information;
- Compromised privacy and confidentiality requirements;
- Storing energy by selfish node and to avoid from cooperation;

- The WSN functionality degradation;
- Network partition by non-cooperate in operations;

F. Attacks based on attacker location

Attacker can be deployed inside or outside the WSN; if the attacker be into the WSN's range, called insider (internal), and if the attacker is deployed out of the WSN's range, called outsider (external). This subsection presented and classified the WSNs' routing attacks based on attackers' location, including:

1) External attacker (outsider): some of the most common features of this type of attacks are:

- External to the network [2, 19] (from out of the WSN range);
- Device: Mote/Laptop class;
- Committed by illegally parties [2, 7];
- Initiating attacks without even being authenticated;

Some of common effects of these attacks are including:

- Jamming the entire communication of the WSN;
- WSN's resources consumption;
- Triggering DoS attacks;

2) Internal attacker (insider): the meaning of insider attacker is:

- Main challenge in WSNs;
- Sourced from inside of the WSN and access to all other nodes within its range [2, 5, 7];
- Authorized node in the WSN is malicious/compromised;
- Executing malicious data or use of cryptography contents of the legitimate nodes [19, 20];
- Legitimate entity (authenticated) compromising a number of WSN's nodes;

Some of most important goals of these attacks type are:

- Access to cryptography keys or other WSN codes;
- Revealing secret keys;
- A high threat to the functional efficiency of the whole collective;
- Partial/total degradation/disruption;

G. Attacks based on attacking devices

Attackers can use different types of devices to attack to the WSNs; these devices have different power, radio antenna and other capabilities. There are two common categories of them, including:

1) Mote-class attacker: mote-class attacker is every one that using devices similar to common sensor nodes; this means,

- Occurring from inside the WSN;
- Using WSN's nodes (compromised sensor nodes) or access to similar nodes/motes (which have similar functionality as the WSN's nodes) [7, 8];
- Executing malicious codes/programs;

Mote-class attacker has many goals, such as:

- Jamming radio link;
- Stealing and access to cryptography keys;

2) Laptop-class attacker: laptop-class attacker is every one that using more powerful devices than common sensor nodes, including:

- Main challenge in WSNs;
- Using more powerful devices by attacker, thus access to high bandwidth and low-latency communication channel;
- Traffic injection [2];
- Passive eavesdrop [19] on the entire WSN by a single laptop-class device;
- Replacing legitimate nodes;

Laptop-class attackers have many effects on WSNs, for example:

- Launching more serious attacks and then lead to more serious damage;
- Jamming radio links on the WSN entirely (by using more powerful transmitter);
- Access to high bandwidth and low-latency communication channel;

H. Attacks based on function (operation)

Routing attacks in WSNs have been classified into three types, based on their main functionality; this subsection presented them, include:

1) Secrecy: its definition and techniques are:

- Operating stealthy on the communication channel;
- Eavesdropping [4, 20];
- Packet replay, spoofing or modification;
- Injecting false data into the WSN [5, 6];
- Cryptography standard techniques can prevent from these attacks;

Goals and effects of this kind of attacks are:

- Passive eavesdrop;
- Packet replication, spoofing or modification;

2) Availability: this class of attacks known as Denial of Services (DoS) attacks; which leads to WSNs' unavailability, degrade the WSNs' performance or broken it. Some of the most common goals and effects of this attacks' category are including:

- Performance degradation;
- The WSN's services destruction/disruption;
- The WSN useless/unavailable;

3) Stealthy: These kinds of attacks are operating stealthy on the communication channel; such as:

- Eavesdropping [2, 8, 20];
- False data injection into the WSN;

The most important effects of these attacks are including:

- Partial/entire degradation/disruption the WSN's services and functionality;

Attack category/	**Types**	**Damage level[1]**	**Ease of identify[2]**	**Attacker presence[3]**

[1] damage level: high (serious or more damage than other type) and low (limitary);

features				
Based on damage level	Active attacker	High	Easy	Explicit
	Passive attacker	Low	Hard	Implicit
Based on attacker location	External (outsider)	Low	Medium	Implicit
	Internal (insider)	High	Hard	Implicit
Based on attacking devices	Mote-class attacker	Low	Hard	Implicit
	Laptop-class attacker	High	Easy	Explicit
Based on attack function	Secrecy	High	Hard	Implicit
	Availability	High	Hard	Both
	Stealthy	High	Hard	Implicit

Table1. Threat model of WSNs

As shown in table1, damage level of routing attacks on WSNs can be high (serious effect on the WSN) or low (limited effect on the WSN); besides, the attackers identification can be easy (possible), medium or hard (impossible), depending on that kind of attack; also the attackers' presence or attacks' effects can be explicit (serious damage) or implicit (for example, eavesdropping).

V. Definitions, strategies and effects of routing attacks on WSNs

WSNs are designed in layered form; this layered architecture makes these networks susceptible and lead to damage against many kinds of attacks. For each layer, there are some attacks and defensive mechanisms. Thus, WSNs are vulnerable against different routing attacks, such as DoS attacks, traffic analysis, privacy violation, sinkhole and other attacks to routing protocols [2, 19]; since in the WSNs, sensor nodes collaborate to each other for routing; the collaboration between sensors is susceptible to routing attacks. Attackers can gain access to routing paths and redirect the traffic, or propagate or broadcast false routing information into the WSNs, or launch DoS attacks against routing. In table2 is presented the definitions of routing attacks on WSNs, and then it classified and compared them to each others based on their strategies and effects.

[2] ease of identify attackers: easy (possible), medium (depending on attack type) and hard (impossible or not as easy to prevent as other ones);
[3] attacker presence or attack's effect: explicit (more powerful attacker, then more serious damage/harm) and implicit;

Attacks/criteria	**Attack definition**	**Attack techniques**	**Attack effects**
Homing	• Regular traffic monitoring and analyzing the messages transferred, communication patterns and sensor nodes activities ⇨ identifying and locate critical resources that provide critical/vital services to the WSN ⇨ launching active attack;	• Regular monitoring and traffic analysis, include rate monitoring attack and time correlation attack; • Plug into the wireless channel within the sender's transmission range; • Using powerful resources or strong devices;	• Identifying, locate and destroy critical resources; • Extracting the sensitive network information; • Launching active attacks (wormhole, blackhole, sinkhole); • Threaten data confidentiality and privacy;
Neglect and greed[4]	• Malicious node drop incoming packets, randomly or arbitrarily (neglectful node); • Malicious node gives undue priority to its own messages (greedy node);	• Selective forwarding and blackhole attacks techniques; • Misusing from routing protocols;	• Consistently degrade or block traffic; • Packet drop/losses; • Influencing/limiting the WSN traffic; • Low reliability;
Rushing	• Quick broadcast the false advertisings of route request through the WSN [16]; • An attacker exploits duplicate suppression in broadcasts to suppress legitimate packets by quickly forwarding its own packets;	• Forwarding route requests more quickly than any normal nodes [16]; • Use of duplicate suppression in routing protocols [16]; • Sending forged or modified route requests to the entire WSN; • Keeping the network interface transmission queues of nearby nodes full; • Employing a wormhole; • Misusing from properties of all on-demand protocols; • Forwarding request without checking signature; • Use of a longer transmission range; • Ignoring MAC layer's delays;	• Discarding correct requests; • Launch other attacks such as blackhole or wormhole; • Partition the network; • Unable to discover any usable/useful routes; • Provide a significant latency advantage; • Strengthening the attackers' position; • Forming/establish a wormhole tunnel;
Gratuitous detour attack	• Making a route through attacker appear longer where a shorter route exists and would otherwise be used, by adding virtual nodes to the route;	• Routing information modification or replication or injection (unauthenticated injection); • Faking routing information; • Discard/ignore routing information; • Misdirection (traffic direction to wrong path);	• Non-cooperation between nodes; • Resources exhaustion; • Routing loops; • Routing inconsistencies; • Traffic attraction/repel; • Network partition; • Misdirection; • Extend or shorten source routes; • Low reliability;
Node malfunction	• Inaccurate data generation [4];	• Malicious data injection;	• Integrity destruction; • Degradation the WSN efficiency; • Taking over the WSN; • Resources exhaustion;
HELLO flood	• Bombing/flooding whole	• Luring sensors;	• Disrupt topology construction;

[4] We can classify this attack based on attack nature (include selective forwarding or blackhole) and based on complexity (contain neglectful mode and greedy mode attack);

	network with routing protocol's HELLO packets [9] (with more energy [4, 7]), that announcing false neighbor status using powerful radio transmitter [10];	• Broadcast high power HELLO message to legitimate nodes [4]; • Forged/false advertising high quality route to sink [10];	• Network and routing confusion/destruction; • Exhausting nodes' energy; • Decrease efficiency and cooperation; • Increase the WSN latency;
Flooding attack[5] or packet replication attack	• Flooding on application layer: exhausting the resources of sensors [21]; • Flooding on routing layer: a node generates and propagates numerous route requests;	• Simple broadcast flooding; • Simple target flooding; • False identity broadcast flooding; • False identity target flooding; • Enforcing additional processing to nodes; • Compromised routing information;	• Resource exhaustion; • Reducing WSN's availability; • Blowing up the traffic statistics of the WSN or a certain node and lead to considerable damage costs;
Sinkhole	• A special selective forwarding attack; • More complex than blackhole attack; • Attracting [4, 9] or draw the all possible network traffic to a compromised node by placing a malicious node closer to the base station [12] and enabling selective forwarding; • Centralizing traffic into the malicious node [18]; • Possible designing another attack during this attack; • Sinkhole detection is very hard[6];	• Luring [2] or compromising nodes [10]; • Tamper with application data along the packet flow path (selective forwarding); • Receiving traffic and altering or fabricating information [12]; • Identity spoofing for a short time; • Using the communication pattern; • Creating a large sphere of influence; • Based on used routing protocol: MintRoute or MultiHopLQI protocol;	• Luring and to attract almost all the traffic; • Triggering other attacks, such as eavesdropping, trivial selective forwarding, blackhole and wormhole; • Usurp the base station's position; • Message modification; • Information fabrication and packet dropping; • Suppressed messages in a certain area; • Routing information modification/fake; • Resource exhaustion;
Blackhole	• A form of selective forwarding attack; • A kind of Denial of Service (DoS) attack that the attacker swallows all the received messages; • Drop all incoming packets [14, 17];	• Dropping all incoming packets from neighboring/children nodes [14]; • Reducing the latency [14] and deceiving/luring the neighboring nodes; • Advertise/broadcast or propagate spoofed/false information such as routing information, to neighboring nodes [17, 21];	• Decreased the throughput of a subset of nodes (especially the neighboring nodes); • Loss blackhole's neighbors; • Network partition; • Packet loss; • Influencing the network traffic; • Limiting or preventing send/receive traffic;
Grey-hole[7]	• Partial blackhole attack; • Similar to the black hole attack except that the malicious node selectively or randomly forwards/drops only some of data packets that they are routed through it, at random intervals to protect from its forged/artificial path; • A kind of Denial of	• Blackhole attack techniques; • Selective forwarding attack techniques; • Protecting from forged path that create by attacker; • Distorting routing information; • Packet modification (TTL); • Modifying the discovered route **in** a ROUTE REPLY; • Making a route that appears	• Impossibility verifying malicious nodes; • Traffic attraction; • Degrade the throughput of a subset of nodes; • WSN partially disruption; • Creating routing loops; • Packet dropping; • Constraining send/receive traffic; • Partition the WSN;

[5] Applications of flooding: constructing routing tree, clock synchronization and information query;
[6] because they use private, invisible and out-of-band channels;
[7] A form of blackhole or selective forwarding attack; based on attacker or grey-hole location: located close to the base station/sink or located at the edge of the WSN; Based on attacker location on WSN: attacker is on the path of data flow or attacker overhears the data flow; Based on node type: operating by compromised node or attractive node;

	Service attack that the attacker receives but does not forward all incoming messages;	longer where a shorter route exists and would otherwise be used;	• Decrease collaboration; • Resources exhaustion;
Wormholes	• Tunneling [4, 10] and replicating messages from one location to another through alternative low-latency links, that connect two or more points (nodes) of the WSN with fast communication medium [21] (such as Ethernet cable, wireless communication or optical fiber), by colluding two active nodes (laptop-class attackers) in the WSN, by using more powerful communication resources than normal nodes [3, 15] and establishing better real communication channels (called tunnel); • Wormhole nodes operate fully invisible [15];	• Compromising/luring nodes with false and forged routing information; • An attacker locates between two nodes and forwards messages between them; • Using out-of-band or high-bandwidth fast [21] channel; • Wormholes may be used along with Sybil attack; • This attack may combines with selective forwarding or eavesdropping;	• Routing disruption/disorder (false routes, misdirection and forged routing); • False/forged routing information; • Confusion and WSN disruption; • Enable other attacks; • Exploiting the routing race conditions; • Change the network topology; • Prevention of path detection protocol; • Packet destruction/alteration by wormhole nodes; • Changing normal messages stream;
Spoofed, altered, or replayed routing information[8]	• Making a path cycle between the source and the destination nodes (so the data message will go around in circle, possibly forever); • Its target is the routing information exchanged between nodes [10]; • A type of DoS attack that Injects fake or false routing information into the WSN;	• Node identity replication/fabrication;; • Generating false and misleading messages; • Spoofing, altering or replaying routing information; • Misdirection; • Unauthenticated injections; • Overflowing routing tables [3]; • Routing table poisoning [3]; • Route cache poisoning [3];	• Network partition; • Misdirection; • Resources exhaustion; • Decrease network lifetime; • False error messages generation; • Low reliability; • Discard routing information; • Wrong routing tables;
Acknowledge spoofing[9]	• An adversary can spoof link layer acknowledgements (ACKs) of overheard packets [10];	• ACKs replication; • Forging/spoofing link layer ACKs of neighbor nodes;	• False view/information of the WSN; • Launch selective forwarding attack; • Packet loss/corruption;
Sybil[10]	• A single node forges multiple identities [10, 19, 24];	• Identity fraud, spoof or duplication [24, 25]; • False/forged information injection (such as routing info) [25]; • Misusing from weak points of geographical [7] and multi-path routing protocols;	• Break the data integrity and accessibility; • Geographical and multipath routing protocols disruption; • Reducing diversity; • Reducing the effectiveness of fault tolerant schemes [19, 24];
Impersonation[11]	• Malicious node impersonates a cluster	• The WSN reconfiguration; • Access to encryption keys and	• Routing information modification;

[8] Also called routing loops/cycles or DoS attacks over the routing protocols or false routing information attack (there are 3 types false routing attacks, that are: overflowing routing tables, routing table poisoning and route cache poisoning);

[9] Attacks on protocols which relay on link layer acknowledgement (ACK); Some WSN routing protocols use link layer acknowledgments (ACKs); the adversary can spoof link layer ACKs of overheard packets (due to broadcast nature of transmission media) to convince other nodes that weak link is strong or dead node is alive;

[10] Different dimensions of Sybil attacks are: communication (direct or indirect), identities (fabricated or stolen) and simultaneity (simultaneous or non-simultaneous);

[11] Also called identity spoofing or node replication [23] or multiple identity attacks; identity spoofing and play the role of other one [23]; the attacker assumes the identity of another node in the network, thus receiving messages directed to the node it fakes;

	leader and lures nodes to a wrong position; • Impersonating a node within the path of the data flow of attacker's interest by modifying routing data or implying itself as a trustworthy communication partner to neighboring nodes in parallel;	authentication information; • Man-in-the-middle attack and fake MAC addresses; • Node replication [23]; • Physical access to the WSN; • False or malicious node attack techniques; • Sybil attacks techniques; • Misdirection/misrouting; • Modifying routing information; • Luring/convince nodes;	• False sensor readings; • Making network congestion or collapse; • Disclose secret keys; • Network partition; • False and misleading messages generated; • Resources exhaustion; • Degrade the WSN performance; • Invasion; • Carrying out further attacks to disrupt operation of the WSN; • Confusion and taken over the entire WSN;
Eavesdropping[12]	• Detecting the contents of communication by overhearing/stealthy attempt to data;	• Interception; • Abusing of wireless nature of WSNs' transmission medium; • Using powerful resources and strong devices, such as powerful receivers and well designed antennas;	• Launching other attacks (wormhole, blackhole); • Extracting sensitive WSN information; • Delete the privacy protection and reducing data confidentiality;
Traffic Analysis	• An attack against privacy (privacy violation); • Regular monitoring, detecting and analyzing the messages transferred, contents of communication patterns and sensor nodes activities [4] ⇨ extracting and revealing the sensitive information ⇨ harming to the WSN;	• Rate monitoring attack techniques; • Time correlation attack techniques; • Compromising the base station or the nodes which they are near to the base station; • Misusing from the wireless nature of WSNs' transmission medium; • Using powerful resources;	• Monitoring and access to the WSN information; • WSN partial disruption/destruction; • Launching other attacks (wormhole and blackhole); • Privacy protection elimination; • Data confidentiality deletion;
Selective forwarding	• In application layer (message selective forwarding): the attacker selectively sends the information of a particular sensor [3]; • In network layer (sensor selective forwarding): the attacker sends/discards the information from selected sensors [3]; • There are 2 modes of this attack: Simple mode attack [10][13] and complex mode attack [10][14];	• In application layer: understanding the semantics of the payload of the application layer packets; but in routing layer: • Reducing the latency and deceiving the neighboring nodes; • Misuse of nodes' faithful (which forward all received messages); • Packet dropping or modification or suppression; • The attacker is on the route of packet transfer in a multi-hop network; otherwise, needs to position himself in the routing path using other attacks (the Sybil, sinkhole and routing table poisoning attack);	• Drop/alter certain messages; • Influencing the WSN traffic; • Impossibility verifying malicious nodes;
Misdirection	• Misrouting the received packets or traffic flows in one direction to a distant node;	• Generating wrong messages; • Routing information modification, fabrication, replication or discard;	• Packets misdirection; • Flooding its network link; • Wrong routing tables (false routing information);

[12] Also called passive information gathering attack; a threat for data confidentiality; the most common attack against privacy; an adversary with powerful resources (powerful receiver and well designed antenna) can gather the data stream from the WSN, if they are not encrypted;
[13] blackhole form that compromised node refuse to forward any packets;
[14] selective form that compromised node forwards/drops certain packets;

	• Forwarding messages to/along wrong paths;	• Internet smurf attacks techniques;	• Non-cooperation; • Resources exhaustion; • Network partition; • Low reliability; • Reducing the WSN's availability;
Denial of Service (DoS) attacks	• A general attack includes several types other attacks in different layers of WSN, simultaneously [28]; • Reducing the WSN's availability [19, 28];	• Physical layer attacks techniques; • Link layer attacks techniques; • Routing layer attacks techniques; • Transport layer attacks techniques; • Application layer attacks techniques;	• Effects of physical layer, link layer, routing layer, transport layer and application layer attacks;

Table2. Routing attacks on WSNs (classification and comparison based on strategies and effects)

VI. Comparison routing attacks on WSNs

WSNs are vulnerable against routing attacks. Therefore, we have to use some techniques to protect data accuracy, network functionality and its availability. As a result, we require establishing security in WSNs with attention to requirements and limitations of these networks.

I. Routing attacks classification based on threat model of WSNs

In this subsection, we have tried to compare the routing attacks of WSNs based on attacks' nature and effects, attackers' nature and capabilities, and WSN's threat model; as shown in following table (table3).

Table3 shows the most important known attacks on WSNs; this table has three columns, including security class, attack threat and WSNs' threat model. Our purpose of security class is the nature of attacks, includes interruption, interception, modification and fabrication. Attack threat shows which security service attacked or security dimension affected, includes confidentiality, integrity, authenticity and availability. The threat model of WSNs has three sub-columns, that they are presenting attackers' features and capabilities, including based on attacker location (internal/insider or external/outsider), based on attacking devices (mote-class or laptop-class) and based on attacks on WSN's protocols, include active attacks and passive attacks; active attacks are targeting availability (packet drop or resource consumption), integrity (information modification) and authenticity (fabrication); passive attacks are aiming confidentiality (interception).

Attacks/features	**Security class**	**Attack threat**	**Threat model[15]**		
			Attacker location	**Attacking device**	**Attacks on WSN's protocols**
Homing	Interception	Confidentiality	External	Laptop	Passive
Neglect and greed	Fabrication	Availability, authenticity	Internal	Mote	Active
Rushing	Modification, fabrication	Availability, integrity, authenticity	External	Laptop	Active
Gratuitous detour	Fabrication	Availability, integrity, authenticity	External	Laptop	Active
Node malfunction	Interruption, fabrication	Availability, authenticity	External	Laptop	Active
HELLO flood	Fabrication	Availability, authenticity	Internal	Mote	Active
Flooding	Modification, fabrication	Availability, integrity, authenticity	Internal	Mote	Active
Sinkhole	Modification, fabrication	Availability, integrity, authenticity	Both	Both	Active
Blackhole	Fabrication	Availability,	Internal	Mote	Active

[15] Threat model: based on attacker location or access level (internal/insider or external/outsider), based on attacking devices (mote-class or laptop-class) and based on damage/attacks on WSN protocols include active attacks (availability (packet drop or resource consumption), integrity (information modification) and authenticity (fabrication)), passive attacks (confidentiality (interception));

		authenticity			
Grayhole	Fabrication, modification	Availability, integrity, authenticity	Internal	Mote	Active
Wormholes	Fabrication, interception	Confidentiality, authenticity	External	Both	Active
Spoofed, altered, or replayed routing information	Fabrication, modification	Integrity, authenticity	Both	Both	Active
Acknowledge spoofing	Fabrication, modification	Integrity, authenticity	Both	Both	Active
Sybil	Modification, fabrication	Availability, authenticity, integrity	Both	Both	Active
Impersonation	Interception, fabrication, modification,	Availability, integrity, confidentiality, authenticity	External	Both	Active
Eavesdropping	Interception	Confidentiality	External	Both	Passive
Traffic Analysis	Interception	Confidentiality	External	Laptop	Passive
Selective forwarding	Modification	Availability, integrity	Both	Both	Active
Misdirection	Modification, fabrication	Availability, integrity, authenticity	Both	Both	Active
Denial of Service (DoS) attacks	Interruption, interception, modification, fabrication	Availability, integrity, confidentiality, authenticity	Both	Both	Active

Table3. WSN's routing attacks classification based on WSNs' threat model

Following figure (figure5) shows the nature of WSN's routing attacks; it compares these attacks based on their nature by presents the percentage of WSNs' routing attacks which based on interruption, interception, modification or/and fabrication; as a result, the nature of the most of these attacks is fabrication (almost 80 percent of them).

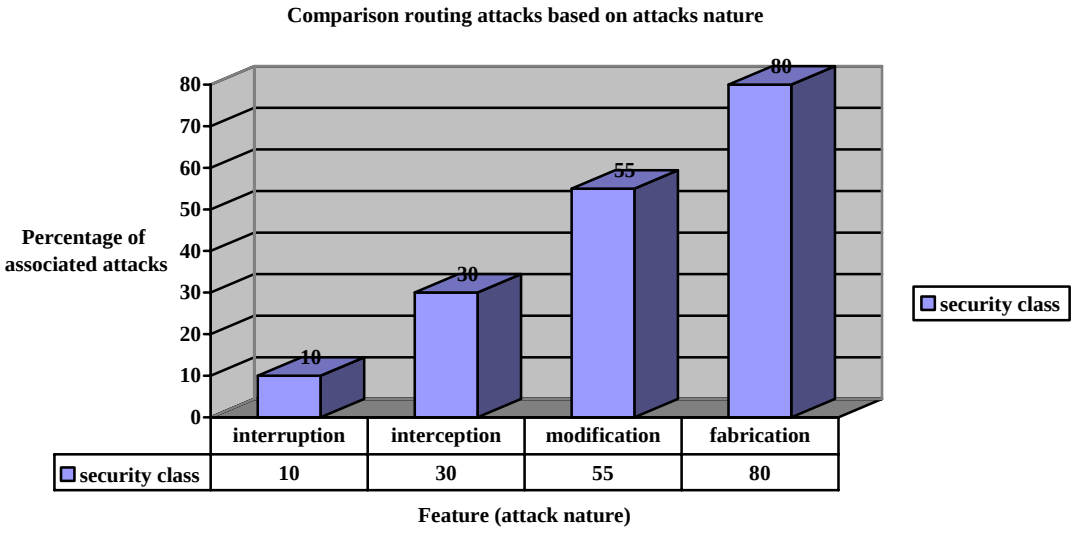


Figure5. Comparison routing attacks based on their nature

Following diagram (figure6) shows a comparison of WSNs' routing attacks based on their security threats factors including confidentiality, integrity, authenticity and availability, in percentage; for example, it presents almost 30 percent of security threat of WSNs' routing attacks is confidentiality and the nature of 80 percent of them is fabrication (fabricating data or identity). As shown in figure6, the aim of the most WSNs' routing attacks is attacking authenticity.

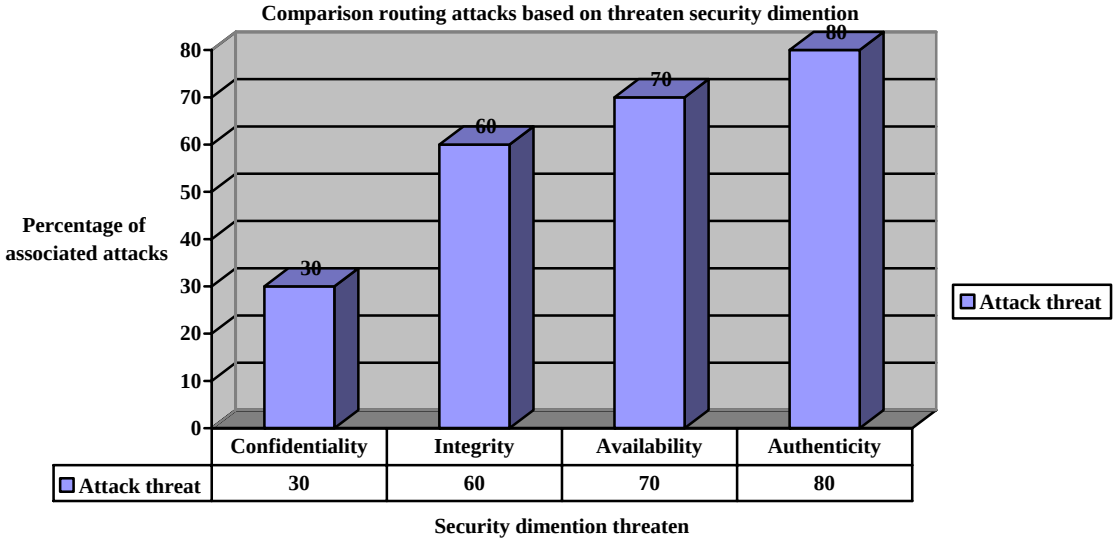


Figure6. Comparison routing attacks based on affected security dimension

Following figure (figure7) shows a comparison routing attacks based on the threat model of WSNs; As shown figure7, the occurred percentage of WSNs' routing attacks, in attacker location, are 25 percent internal, 40 percent external and 35 percent from both; i.e. most of WSNs' routing attacks are occurring from out of WSNs' range and attackers can trigger them by mote-class or laptop-class devices. Also, it presents most of routing attacks on WSNs are active, except homing, traffic analysis and eavesdropping; i.e. almost 85 percent of WSNs' routing attacks are active. Besides, figure7 shows most attacks on routing layer of WSNs are external attacks.

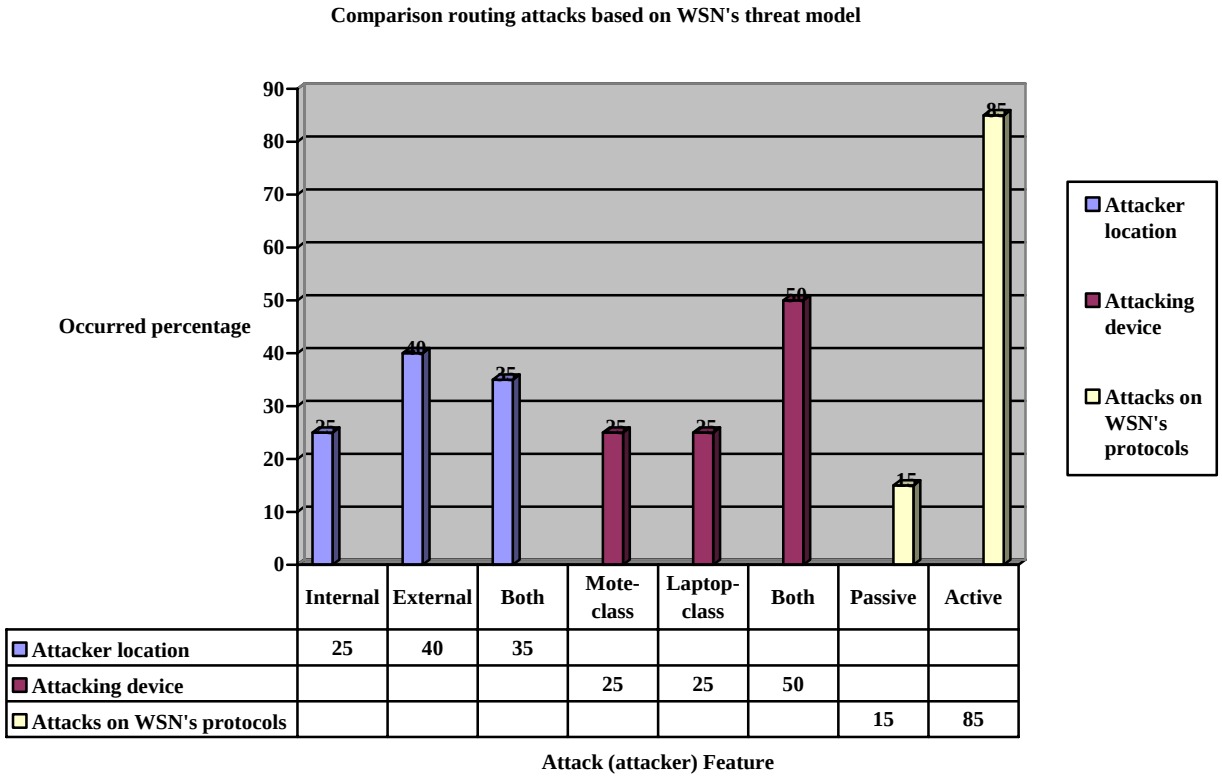


Figure7. Comparison routing attacks based on the threat model

J. Routing attacks comparison based on their goals and results

In routing layer, attackers can disrupt the WSN's functionality by tampering the routing services such as modifying routing information and replicating data packets. As shown in table4, it categorizes the routing attacks of WSNs, based on their goals, effects and results. Also table4 compares WSNs' routing attacks based on attack or attacker purpose (including passive eavesdrop, disrupt communication, unfairness, authorization and authentication), requirements technical capabilities (such as radio, battery, powerful receiver/antenna and other high-tech and strong attacking devices), vulnerabilities, main target and final result of attacks. Besides, the contributors of all following routing attacks (shown in table4) are one or many compromised motes, pc or laptop devices on WSNs. The vulnerabilities of these attacks can be physical (hardware), logical or their both; Attacks' main target may be physical (hardware), logical (lis: logical-internal services or lps: logical-provided services) or their both. Final result of these attacks is including passive damage, partial degradation of the WSN functionality and total broken of the WSN's services or functionality.

Attacks/ features	**Purpose**[16]	**Technical capability**	**Vulnerability**[17]	**Main target**[18]	**Final result**[19]
Homing	Passive eavesdrop of data	Radio; powerful resources and strong devices[20]	Logical	lps	Passive damage; PTDB[21]
Neglect and greed	Unfairness	-	Logical	lps	PTDB
Rushing	Unfairness	-	Logical	lis; lps	PTDB
Gratuitous detour	Unfairness	-	Logical	lps	PTDB
Node malfunction	Unfairness	-	Logical	lis; lps	PTDB
HELLO flood [1]	Unfairness	Radio	Logical	lps	PTDB
Flooding [1]	Unfairness	Battery	Logical	lis	PTDB
Sinkhole [1]	Unfairness	-	Logical	lps	PTDB
Blackhole	Unfairness	-	Logical	lps	PTDB
Grayhole	Unfairness	-	Logical	lps	PTDB
Wormholes [1]	Unfairness; to be authenticated; to be authorized	-	Logical	lps	Passive eavesdrop; PTDB
Spoofed, altered, or replayed routing information	Unfairness	-	Logical	lps	PTDB
Acknowledge spoofing	Unfairness	-	Logical	lps	PTDB
Sybil [1]	Unfairness	-	Logical	lps	PTDB
Impersonation	All purpose	Time and high-tech equipments	Logical; physical	Physical; Logical (lis and lps)	Passive damage; PTDB
Eavesdropping	Passive eavesdrop of data	Powerful resources and strong devices	Logical	lps	Passive damage; partial degradation
Traffic Analysis	Passive eavesdrop of data	Powerful resources and strong devices	Logical	lps	Passive damage; PTDB
Selective forwarding [1]	Unfairness	-	Logical	lps	PTDB
Misdirection	Unfairness	Battery	Logical	lis	PTDB
Denial of Service (DoS) attacks	All purpose	Radio; battery; time and high-tech equipments	Logical; physical	Physical; Logical (lis and lps)	Passive damage; PTDB

Table4. Routing attacks comparison based on attacks' goals and their results

[16] Purpose: passive eavesdrop, disrupt communication, unfairness, to be authorized, to be authenticated;
[17] Vulnerabilities: physical (hardware), logical;
[18] Main target: physical (hardware), logical (lis: logical-internal services or lps: logical-provided services);
[19] Final result: passive damage, partial degradation of the WSN duty, service broken for the entire WSN (partial or entire degradation/disruption of the services/resources/functionality of the WSN);
[20] such as powerful receiver and well designed antenna;
[21] PTDB: Partial/Total Degradation/Broken;

Following figure (figure8) shows that how much percentage of WSNs' routing attacks are happened by targeting the fairness, confidentiality, authentication, authorization and disrupt communication on WSNs' functionalities, services and resources; for example, almost 90 percent of these attacks are aiming the fairness of WSNs, and then they lead to unfairness.

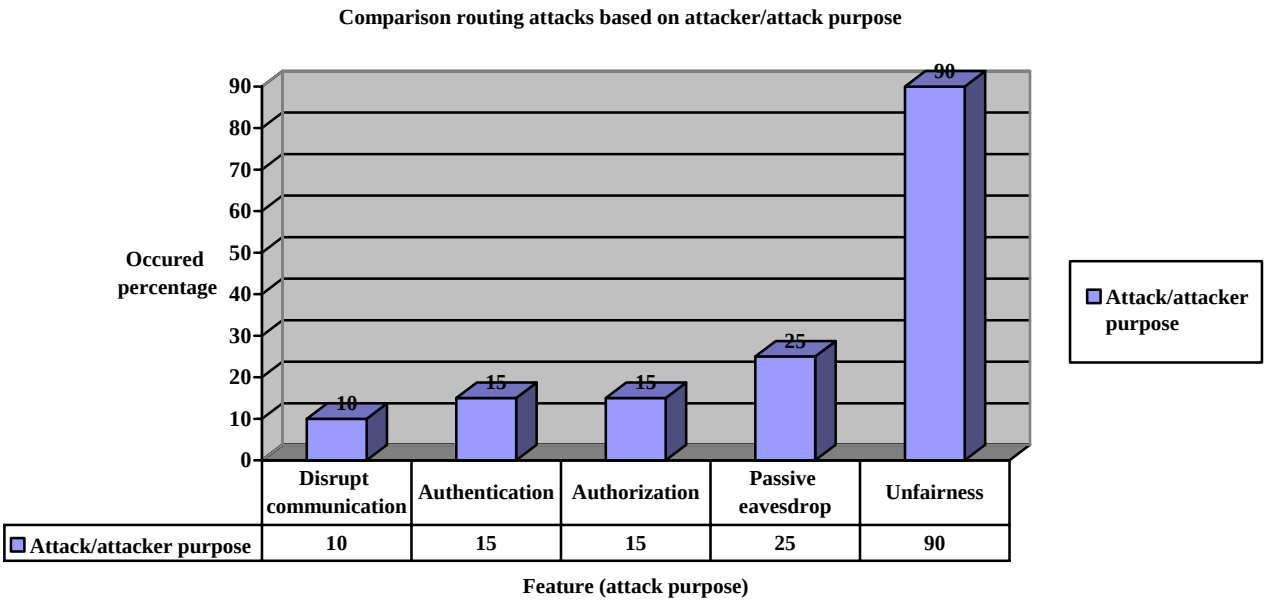


Figure8. Comparison routing attacks based on attacks' purpose

Figure9 is presenting the percentage of every one of kinds of routing attacks vulnerabilities and their main target on WSNs, including: 10 percent of them are attacking the WSNs' hardware, 30 percent of them are aiming the WSNs' logical-internal services and 95 percent are targeting the logical-provided services by WSNs. Thus, most routing attacks on WSNs have logical vulnerabilities and only almost 10 percent of them have physical harm/effects.

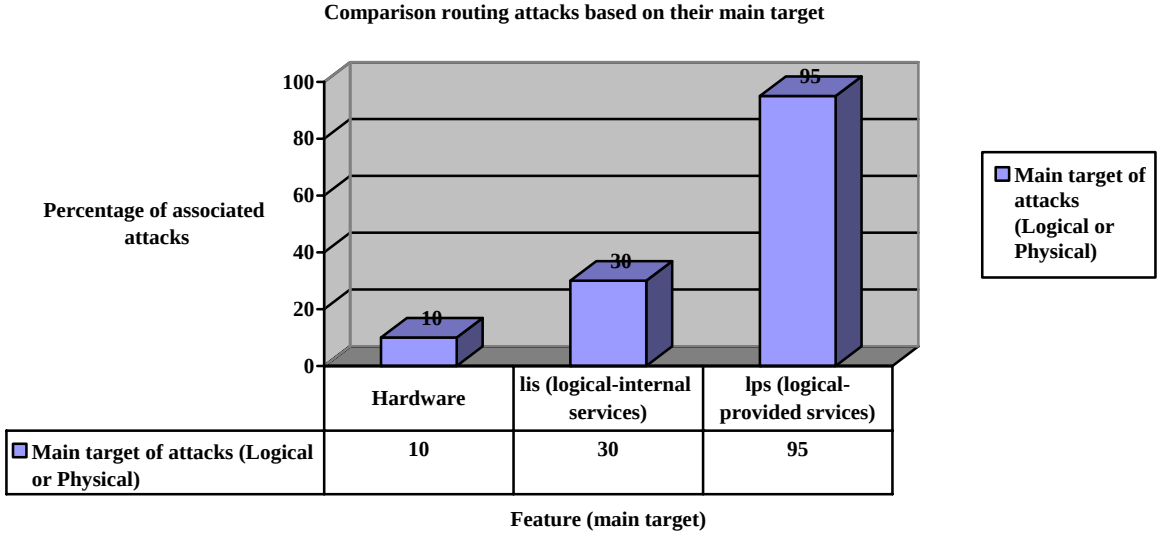


Figure9. Comparison routing attacks based on their main target

K. Detection and defensive strategies of WSNs' routing attacks

In following table (table5) a classification and comparison of detection and defensive techniques of WSNs' routing attacks is presented.

Attacks/criteria	Detection methods	Defensive mechanisms

Homing	• Misbehavior detection techniques;	• Access control; • Reduction in sensed data details; • Distributed processing; • Strong encryption techniques; • Hiding use of shared cryptographic keys;
Neglect and greed	• Misbehavior detection techniques;	• Multi-path routing; • Sending redundant messages; • Probing, redundancy [2] and regular monitoring; • Using other possible routes; • Dynamically and probabilistic pick packet's next hop; • Using combinational methods[22]; • Adopt multi-hop routing and bidirectional link verification;
Rushing Attack	• Evaluating the Route Discovery [16]; • Misbehavior detection techniques;	• Removing delays; • A set of generic mechanisms that together defend against the rushing attack, are [16]: Secure Neighbor Detection, Secure Route Delegation and Randomized Route Request forwarding;
Gratuitous detour attack	• Tree-path routing protocols; • A hop count limit;	• Central certificate authority [23]; • Pair-wise authentication; • Network layer authentication; • Adopt validation techniques;
Node malfunction	• Misbehavior detection techniques;	• Strong authentication, authorization and access control; • Limiting/restricting the number of nodes' neighbors;
HELLO flood	• Misbehavior detection techniques;	• Suspicious node detection by signal strength [2]; • Restricting the number of nodes' neighbors; • Authentication, link layer encryption and global shared key mechanisms[24];
Flooding attack or packet replication attack	• False routing information detection[25]; • Wormhole detection[26];	• Client puzzles [2]; • AODV (Ad hoc On-demand Distance Vector) protocol [21]; • Limiting the number of node's connections; • Routing access restriction[27]; • Key management; • Secure routing [5];
Sinkhole attacks	• False routing information detection [3, 18]; • Cooperating neighboring nodes to each other [14, 18]; • Tree structure and verify by tree [14, 17, 18]; • Verify by Visual Geographical Map;	• Detection on MintRoute [2]; • Geographical routing protocols; • Scalability; • Probabilistic next hop selection (dynamically probabilistic select packet's next hop); • leveraging global knowledge[28] and learning global map (if nodes are static and at known location); • Verifying and to trust information that advertised of neighboring nodes; • Authentication [17], link layer encryption and global shared key techniques; • Routing access restriction (R) [3, 5]; • Wormhole detection (W) [3, 5]; • Key management (K); • Secure routing (S) [3, 5];
Blackhole attack	• Sinkhole attack detection methods;	• Authorization and monitoring[2]; • Redundancy; • Using another route; • Multipath routing [17];

[22] multipath routing and probabilistic routing dynamically;
[23] Building a central certificate authority to keep a record (information) of each sensor node's information such as location;
[24] Multi-path routing, identity verification (node authentication by base stations or create pair-wise shared key for message authentication), bidirectional link verification and authenticated broadcast;
[25] using misbehavior detection methods such as watchdogs or IDS or reputation;
[26] use of techniques such as synchronized clocks, directional antennas and multi-dimensional scaling;
[27] multipath routing; using authentication techniques include: end to end and hop to hop authentication;
[28] mapping entire network topology by this information and continuously or periodically update the information of base station; misbehavior and serious changes in topology show a compromised node; learning global map (if nodes are static); place nodes at known locations;

		• Using combinational method: multipath routing with random selection of paths to destination; • Adopt multi-hop routing and bidirectional link verification [17]; • Defensive mechanisms of sinkhole attack, except learning global map, scalability, geographical routing protocols and detection on MintRoute;
Grey-hole attack	• False routing information detection; • Cooperating neighboring nodes to each other;	• Defensive mechanisms o blackhole attack, except redundancy and leveraging global knowledge;
Wormholes	• False routing information detection; • Wormhole detection [15]; • Combinational methods [15][29]; • Packet leashes techniques [21, 27];	• Packet leach/leashes techniques [21, 27][30]; • MAD protocol and OLSR protocol [21]; • Directional antennas [26]; • Multi-dimensional scaling algorithm (scalability); • Using local neighborhood information; • DAWWSEN protocol [2][31]; • Designing proper routing protocols (clustering-based and geographical routing protocols); • leveraging global knowledge; • Verifying information that announce of neighbor nodes; • Graphical Position System [26, 27]; • Ultrasound [26]; • Global clock synchronization[32]; • Combinational methods (such as radio waves and ultrasound); • Authentication, link layer encryption and global shared key techniques; • (R), (W), (K), (S) [3, 5];
Spoofed, altered, or replayed routing information	• False routing information detection; • Using tree-path routing protocols; • Using a hop count limit;	• Central certificate authority; • Pair-wise authentication ; • Network layer authentication (guard against unauthenticated injections); • Adopt validation techniques; • Authentication, link layer encryption and global shared key techniques; • (R), (W), (K), (S) [3];
Acknowledge spoofing	• Misbehavior detection techniques;	• Using another route[33]; • Authentication, link layer encryption and global shared key techniques;
Sybil attack	• False identity detection techniques; • False routing information detection;	• Certificate Authority (CA) and utilizing identity certificates; • Limiting the number of node's neighbors [25]; • Physical protection of devices; • Changing key regularly; • Resetting devices and changing session keys (network layer); • Authentication, link layer encryption [2] and global shared key techniques [25]; • Identity protection (Direct validation and Indirect validation)[34]; • (R), (W), (K), (S) [3, 5];
Impersonation	• False identity detection techniques (misbehavior	• Strong and proper authentication techniques; • Using strong data encryption;

[29] such as radio waves and ultrasound, measuring distance between nodes and comparing packet send and receive time with threshold;
[30] Geographical leashes and Temporal leashes ⇨ Physical monitoring of field devices and regular network monitoring by using source routing; monitoring system may use packet leach techniques;
[31] suspicious node detection by signal strength; a proactive routing protocol based on the hierarchical tree construction;
[32] Using tight clock synchronization, but unfeasible for the majority of WSNs;
[33] Using different path to retransmit the messages;
[34] using cryptography-based authentication or false identity detection techniques such as radio resource test (Sybil attack); position verification (detecting immobile attackers); code attestation (differing executing code on malicious/compromised node with/rather than normal nodes ⇨ detecting attackers by validating executing code on nodes); sequence checking; identity association (associating node identity with used keys on communication by that node);

	detection techniques); • False routing information detection; • Collision detection techniques;	• Secure routing protocols; • Central certificate authority; • Pair-wise authentication; • Network layer authentication; • Adopt validation techniques; • Identity protection; • Link layer encryption; • Limiting the rate of MAC requests; • Use of small frames for each packet;
Eavesdropping	• Eavesdropping is a passive behavior, thus it is rarely detectable; • Misbehavior detection techniques;	• Access control; • Reduction in sensed data details; • Distributed processing; • Access restriction; • Strong encryption techniques;
Traffic Analysis	• Misbehavior detection techniques;	• Access control; • Reduction in sensed data details; • Distributed processing; • Strong encryption techniques; • Sending dummy packets continuously and regular monitoring the WSN;
Selective forwarding	• False routing information detection; • Malicious node detection techniques;	• Regular network monitoring; • Using another route; • Dynamically pick packet's next hop from a set of candidates; • Combinational methods[35]; • Authentication, link layer encryption and global shared key techniques; • Data integrity protection; • Data confidentiality protection; • (R), (W), (K), (S) [3];
Misdirection	• Misbehavior detection techniques; • Hierarchical routing mechanism; • Tree-path routing protocols; • Using a hop count limit;	• Using hierarchical routing mechanism[36]; • Authorization [2]; • Monitoring [2]; • Central certificate authority; • Pair-wise authentication; • Network layer authentication; • Adopt validation techniques; • Acknowledgment verification;
Denial of Service (DoS) attacks	• Detection methods of physical layer, link layer, routing layer, transport layer and application layer attacks;	• Defensive mechanisms of physical layer, link layer, routing layer, transport layer and application layer attacks;

Table5. Routing attacks on WSNs (classification based on detection and defensive mechanisms)

[35] combine link layer multipath routing and probabilistic routing dynamically (random/probabilistic selection/choose of paths to destination dynamically);
[36] Egress filtering approach;

VII. Conclusion

Security is a vital requirement and complex feature to deploy and extend WSNs in different application domains. The most security routing attacks are targeting WSN security dimensions such as integrity, confidentiality, authenticity and availability.

In this paper, we analyze different dimensions of WSN's security, present a wide variety of WSNs' routing attacks and classify them; our approach to classify and compare the WSN's routing attacks is based on different extracted features of WSN's routing layer, attacks' and attackers' properties, such as the threat model of WSNs, routing attacks' nature, goals and results, their strategies and effects and finally their associated detection and defensive techniques against these attacks to handle them, independently and comprehensively. Table6 presents how much percentage of WSNs' routing attacks are occurring based on any one attacks' classifications features. Figure10 shows most affected features of WSNs' routing attacks. Our most important findings are including:

- Discussion typical WSNs' routing attacks along with their characteristics, in comprehensive;
- Classification and comprehensive comparison of WSNs' routing attacks to each other;
- Link layer encryption and authentication mechanisms can protect against outsiders, mote-class attackers, bogus routing information, Sybil, HELLO flood and acknowledgement spoofing attacks;
- Geographical routing protocols are resistant against Sybil, wormhole and sinkhole attacks;
- Encryption is not enough and inefficient for inside attacks and laptop-class attackers; but clustering protocols can provide most secure solutions against inside attacks and compromised nodes;
- The routing attacks are often launching combinational (intra-layer or cross-layer);
- The different kinds of routing attacks may be used same strategies;
- The same type of defensive mechanisms can be used in multiple routing attacks, such as misbehavior detection;
- The accuracy of solutions against routing attacks depends on the characteristics of the WSN's application domain;
- As presented in table6, 55 percent of routing attacks' nature is modification; 30 percent of routing attacks threaten confidentiality, etc;
- As shown in figure10, the nature of 80 percent of WSNs' routing attacks is fabrication; 80 percent of them are targeting authenticity; most of these attacks are out of the WSNs' range (external: 40 percent) and lead to high-level damages (active attacks: 85 percent); 90 percent of attacks' purpose is unfairness; 95 percent of routing attacks' main target is WSNs' logical provided services;

This work makes us enable to identify the purpose and capabilities of the attackers; also the goal, final result and effects of the attacks on the WSNs' functionality. The next step of our work is considering other attacks on WSNs. We hope by reading this paper, readers can have a better view of routing attacks and aware from some defensive techniques against them; as a result, they can take better and more extensive security mechanisms to design secure WSNs.

Attack or attacker feature		**Criteria**	**Percent (percentage of occurred)**
Security class		Interruption	10
		Interception	30
		Modification	55
		Fabrication	80
Attack threat		Confidentiality	30
		Integrity	60
		Availability	70
		Authenticity	80
Threat model	Attacker location	Internal	25
		External	40
		Both	35
	Attacking device	Mote-class	25
		Laptop-class	25
		Both	50
	Attacks on WSN's protocols	Passive	15
		Active	85
Attacker purpose		Disrupt communication	10
		Authentication	15
		Authorization	15
		Passive eavesdrop	25
		Unfairness	90
Attack main target		Physical (hardware)	10
		Logical-internal services	30
		Logical-provided services	95

Table6. Occurred percentage of each attacks' classification features

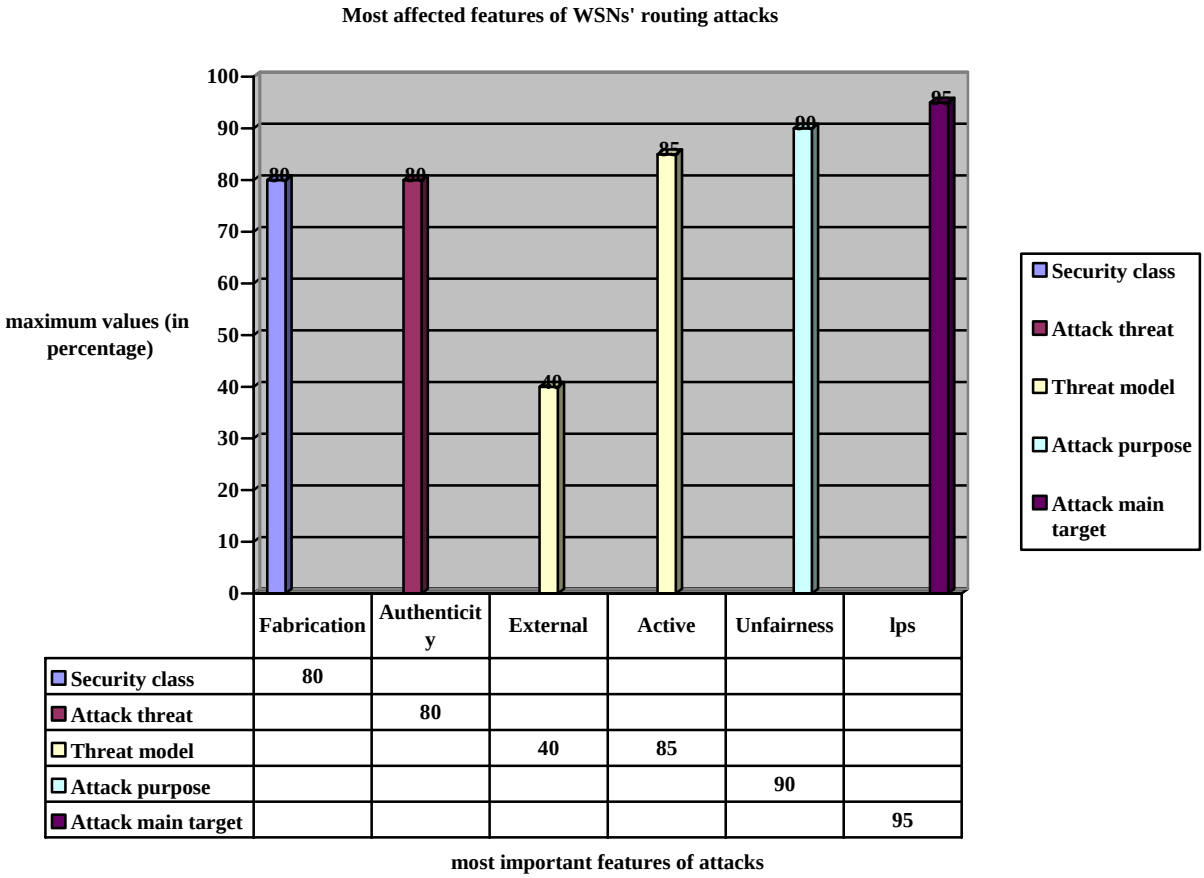


Figure10. Most affected features (have maximum values) on WSNs' routing attacks

VIII. Future works

We also can research about following topics:

- Securing wireless communication links against eavesdropping, traffic analysis and DoS attacks;
- Resources limitations techniques of WSNs;
- Using public key cryptography and digital signature in WSNs (of course with attention to WSN's constraints);
- Countermeasures for combinational routing attacks;
- Designing proper routing protocols for WSNs;
- Optimizing existing WSNs' routing protocols;

References

[1] W. Znaidi, M. Minier, J.P. Babau. "An Ontology for Attacks in Wireless Sensor Networks". INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE (INRIA), Oct 2008.

[2] K. Sharma, M.K. Ghose. "Wireless Sensor Networks: An Overview on its Security Threats". IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs, CSE Department, SMIT, Sikkim, India, 2010.

[3] K. Xing, S. Sundhar, R. Srinivasan, M. Rivera, J. Li, X. Cheng. "Attacks and Countermeasures in Sensor Networks: A Survey". Computer Science Department, George Washington University, Springer, Network Security, 2005.

[4] T.A. Zia. "A Security Framework for Wireless Sensor Networks". Doctor of Philosophy Thesis, The School of Information Technologies, University of Sydney, Feb 2008.

[5] M. Saxena. "Security in Wireless Sensor Networks: A Layer-based Classification". Department of Computer Science, Purdue University.

[6] Z. Li, G. Gong. "A Survey on Security in Wireless Sensor Networks". Department of Electrical and Computer Engineering, University of Waterloo, Canada.

[7] A. Dimitrievski, V. Pejovska, D. Davcev. "Security Issues and Approaches in WSN". Department of computer science, Faculty of Electrical Engineering and Information Technology, Skopje, Republic of Macedonia.

[8] J. Yick, B. Mukherjee, D. Ghosal. "Wireless Sensor Network Survey". Elsevier's Computer Networks Journal 52 (2292-2330), Department of Computer Science, University of California, 2008.

[9] G. padmavathi, D. Shanmugapriya. "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks". International Journal of Computer Science and Information Security (IJCSIS), vol. 4, No. 1& 2, Department of Computer Science,

Avinashilingam University for Women, Coimbatore, India, 2009.
[10] C. Karlof, D. Wagner. “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”. Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, In First IEEE International Workshop on Sensor Network Protocols and Applications; University of California at Berkeley, Berkeley, USA, 2003.
[11] A. Perrig, R. Szewczyk, V. Wen, D. culler, D. Tygar. “SPINS: Security Protocols for Sensor Networks”. Wireless Networking ACM CCS, 2003.
[12] I. Krontiris, T. Giannetsos, T. Dimitriou. “Launching a Sinkhole Attack in Wireless Sensor Networks, the Intruder Side”. Athens Information Technology, Peania, Athens, Greece.
[13] A. Perrig, J. Stankovic, D. Wagner. “Security in Wireless Sensor Networks”. In Communications of the ACM Vol. 47, No. 6, 2004.
[14] A. Saini, H. Kumar. “Comparison between Various Black Hole Detection Techniques in MANET”. Panjab University, Chandigarh, National Conference on Computational Instrumentation (NCCI), Mar 2010.
[15] R. Maheshwari, J. Gao, S. R. Das. “Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information”. IEEE INFOCOM, Alaska, 2007.
[16] Y. Hu, A. Perrig, D.B. Johnson. “Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols”. Carnegie Mellon University, Rice University, San Diego, California, USA, Sep 2003.
[17] I. Ullah, S.U. Rehman. “Analysis of Black Hole attack On MANETs Using Different MANET Routing Protocols”. Master Thesis, Electrical Engineering, Thesis no: MEE-2010-2698, School of Computing Blekinge Institute of Technology, Sweden, Jun 2010.
[18] C. Tumrongwittayapak, R. Varakulsiripunth. “Detecting Sinkhole Attacks in Wireless Sensor Networks”. ICROS-SICE International Conference, 2009.
[19] Y. Zhou, Y. Fang, Y. Zhang. “Security Wireless Sensor Networks: A Survey”. IEEE Communication Surveys, 2008.
[20] Y. Wang, G. Attebury, B. Ramamurthy. “A Survey of Security Issues in Wireless Sensor Networks”. IEEE Communication Surveys, 2006.
[21] R.H. Khokhar, M.A. Ngadi, S. Mandala. “A Review of Current Routing Attacks in Mobile Ad Hoc Networks”. Faculty of Computer Science and Information System, Department of Computer System & Communication, University Technology Malaysia (UTM), Malaysia.
[22] T. Kavitha, D. Sridharan. “Security Vulnerabilities in Wireless Sensor Networks: A Survey”. Journal of Information Assurance and Security, 2009.
[23] B. Parno, A. Perrig. “Distributed Detection of Node Replication Attacks in Sensor Networks”. Carnegie Mellon University.
[24] J.R. Douceur. “The Sybil Attack”. Proc. 1st ACM Int’l. Wksp. Peer-to-Peer Systems, 2002.
[25] J. Newsome, E. Shi, D. Song, A. Perrig. “The Sybil Attack in Sensor Networks: Analysis & Defenses”. Center for Computer and Communications Security, 2004.
[26] L. Hu, D. Evans. “Using Directional Antennas to Prevent Wormhole Attacks”. In Network and Distributed System Security Symposium (NDSS), 2004.
[27] Y. Hu, A. Perrig, D. Johnson. “Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks”. Proc. 22nd Annual Joint Conference of the IEEE Computer and Communications Societies, 2003.
[28] A. Wood, J. Stankovic. “Denial of Service in Sensor Networks”. IEEE Computer Mag., 2002.

Author Biographies

S. Mohammadi is a former senior lecturer at the University of Derby, UK. He also used to be a Network consultant in the UK for more than fifteen years. He is currently a lecturer in the University Of Khajeh, Nasir, Iran. His main research interests and lectures are in the fields of Networking, Data Security, Network Security, and e-commerce. He may be reached at Mohammadi@kntu.ac.ir or smohammadi40@yahoo.com.

Reza Ebrahimi Atani was born in 1980. He received the B.S. degree in electrical engineering from the University of Guilan in 2002 and the M.Sc and PhD degrees in electronics from Iran University of Science and Technology in 2004 and 2010 respectively. Since 2010, he is an assistant professor in Computer Engineering Department at the University of Guilan. His current research interests include stream cipher design and cryptanalysis, cryptographic hardware and embedded system (CHES), side channel attacks (Power and fault attacks), and design of VLSI circuits.
rebrahimi@guilan.ac.ir.

H. Jadidoleslamy is a Master of Science student at the Guilan University in Iran. He received his Engineering Degree in Information Technology (IT) engineering from the University of Sistan and Balouchestan (USB), Iran, in September 2009. He will receive his Master of Science degree from the University of Guilan, Rasht, Iran, in March 2011. His research interests include Computer Networks (especially Wireless Sensor Network), Information Security, and E-Commerce. He may be reached at tanha.hossein@gmail.com.